修 士 論 文 の 和 文 要 旨

研究科・専攻	大学院　情報理工学研究科　　総合情報学専攻　博士前期課程		
氏　　名	中津　大介	学籍番号	1030069
論 文 題 目	AES 暗号ハードウェアに対する電力解析の精度向上		

要　　旨

1999 年に Kocher, Jaffe と Jun によって提案されたサイドチャネル攻撃（SCA）に端を発し，これまでに数多くの SCA の攻撃と対策の研究成果が報告されている．特によく議論される攻撃として，電力解析攻撃や電磁波解析攻撃などのパッシブ攻撃が存在する．パッシブ攻撃は，暗号処理中のデバイスから漏れ出すサイドチャネル情報（e.g. 電力消費量，電磁波，音等）を解析して秘密情報を特定する．特に Kocher, Jaffe と Jun が提案した差分電力解析(DPA) 攻撃は，電力解析攻撃の一つであり，電力波形を統計処理して部分鍵を効率良く特定する強力な攻撃である．相関電力解析（CPA）攻撃は，ハミング距離モデルを利用して中間値と電力消費量の相関係数を計算し，部分鍵を特定する攻撃である．

本研究では，複数の電力波形を統計処理する SCA 手法に焦点を絞り，電力解析の精度向上について議論する．本研究の成果は，以下の 3 つに集約される．1 つ目は，連続する複数ラウンドの電力波形を利用した CPA 攻撃の提案，適用によって攻撃効率の向上に成功したことである．2 つ目は，実測値に基づく電力モデルの提案，適用によって従来の理論的な電力モデルと比較して，攻撃効率を向上させたことである．3 つ目は，上記の 2 つの成果から得た知見を用いて，DPA contest v2 と呼ばれる世界コンテストで最も強力な電力解析攻撃プログラムを作成したことである．